UNM Physics 452/581: Introduction to Quantum Information, Problem Set 1, Fall 2007

Instructor: Dr. Landahl
Issued: August 28, 2007
Due: September 4, 2007

Do all of the problems listed below. Hand in your problem set at the beginning of class on the desk at the front of the classroom or after class in the box in the Physics and Astronomy main office by 5 p.m. **Please put your name and/or IQI number number on your assignment**, as well as the course number (Physics 452/581). Please show all your work and write clearly. Credit will be awarded for clear explanations as much, if not more so, than numerical answers. Avoid the temptation to simply write down an equation and move symbols around or plug in numbers. Explain what you are doing, draw pictures, and check your results using common sense, limits, and/or dimensional analysis.

1.1 Pgate mania

(a) In class, I gave examples of matrix representatives for some reversible pgates. However, nowhere did I say that pgates had to be reversible! Write down pgate matrices for the irreversible gates AND, OR, and FANOUT. From these examples and what we covered in class, what property do you think a pgate has to satisfy to be reversible?

(b) The Fredkin gate (named for Ed Fredkin) is a reversible three-bit gate that swaps the second two bits if and only if the first bit is a 1. In other words, it is a controlled-SWAP gate. It turns out that, like the Toffoli gate TOF, the Fredkin gate is also universal for classical computation. Clearly, then, each gate must be able to simulate the other. (i) What is the fewest number of Fredkin gates needed to simulate a Toffoli gate? (ii) What is the fewest number of Toffoli gates needed to simulate a Fredkin gate? In both cases, give an example circuit achieving this minimum. (Need a hint? Read Nielsen & Chuang Sec. 3.2.5 and/or Preskill's notes Sec. 6.1.)

(c) It is possible to define pgates for more general objects called pdits, where a pdit is nothing more than a d-dimensional vector of probabilities. An example of a pdit gate is a generalization of the CNOT gate called the controlled-sum gate CSUM, which maps $(i, j) \mapsto (i, i \oplus j)$, where now $\oplus$ means addition modulo d. (i) Write down pgate matrices for the CSUM gate for $d = 3$ and $d = 4$. (ii) Write down inverses for these gates.

1.2 Something is rotten in the state of Denmark.

Prince Hamlet sets out to play a trick on his buddies Rosencrantz and Guildenstern. Knowing that Rosencrantz always chooses heads on a coin toss and that Guildenstern always chooses tails, Hamlet prepares two sets of biased coins that will make him likely to win every coin toss with them. Hamlet puts the heads-biased coins in one of his pockets and the tails-biased coins in the other. His plan is to draw coins from the appropriate pocket whenever a coin-toss situation arises, assuring he will win most of the time.

The heads-biased coins are 90% heads and 10% tails, and the tails-biased coins are 0% heads and 100% tails. So in other words, what Hamlet has jingling in one pocket are pbits that are in the state $\vec{\mathbf{p}} = [0.9\ 0.1]^T$ and in the other pocket pbits that are in the state $\vec{\mathbf{q}} = [0\ \ 1]^T$. (Perhaps more accurately, these coins take on those pbit values in mid-flip).

Tragedy befalls Hamlet. He forgets which pocket has which kind of coin in it! He doesn't even have an inkling as to what the correct pockets are. But ever-resourceful, he has a plan. He will take a coin out of one of his pockets and flip it. If the result is heads, he'll guess that pocket contains the heads-biased coins, and if the result is tails he'll guess that pocket contains the tails-biased coins. He'll then use that information to carry out his con as planned.

After these preparations, Hamlet visits his friends, whereupon Rosencrantz soon challenges Hamlet to flip a coin for the value of the coin itself. Tragedy befalls Hamlet—again. Hamlet loses the coin toss. In payment, Hamlet gives Rosencrantz the coin that failed him. Hamlet returns to the castle and broods, as usual, but for Rosencrantz and Guildenstern, antics ensue.[1]

(a) What is the probability that Hamlet erroneously identified the wrong pocket? [Do not take into account the fact that Hamlet lost the actual coin toss—this is merely a question about his testing process.] (Hint: Introduce a new pbit $\vec{\pi} = [\pi_p\ \pi_q]^T$ that is a "prior" probability on which pbit is in which pocket. Use it with Bayes' rule and a little thinking to determine the answer.)

(b) If Hamlet had coins that were 96% heads, 4% tails and 4% heads, 96% tails, what would the probability be that he erroneously identified the wrong pocket?

The error probability function you developed to answer parts a and b is an operational measure of pbit distinguishability. You should find that in one case the contents of Hamlet's pockets are more distinguishable than the other. Let's see if this measure of distinguishability can be amplified. Suppose that Hamlet flipped two coins from the same pocket in an attempt to be more certain of which pocket held which kind of coin.

(c) For the 90%/10% and 0%/100% coins, what is the probability that Hamlet erroneously identified the wrong pocket in this two-flip scenario? (Note: Hamlet makes his decision based on which coin is most likely to give the results he observed. So if he sees heads-heads he obviously will decide he is drawing from the heads-biased-coin pocket and if he sees tails-tails he will obviously decide he is drawing from the tails-biased-coin pocket. If he sees heads-tails or tails-heads, then he guesses the coin that is most likely to give that sequence of outcomes. If these probabilities are different, then his decision is clear. If they are the same, then he is forced to guess based on his prior probability assessment as to which pocket is which.)

(d) For the 96%/4% and 4%/96% coins, what is the error probability?

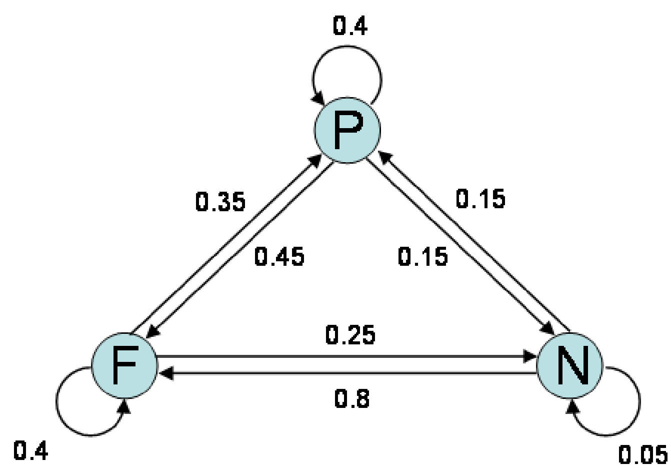
(e) After the two coin-flip test, which pair of pbits is more distinguishable? Explain. (In other words, the more distinguishable of parts (a) and (b) has the smaller error probability and the more distinguishable of parts (c) and (d) has the smaller error probability (Which?). How do these comparisons compare to each other? (I.e., (a)-(b) vs. (c)-(d).) How do you

[1] To see what happens next, read or see Tom Stoppard's play, *Rosencrantz and Guildenstern are Dead.*

make sense of this result? Perhaps thinking of other examples from everyday life will lead you to a clarifying analogy.)

1.3 So teach, when's the homework due?

A physics professor, not wanting to be predictable, decided to assign problem sets in a probabilistic fashion. On the first day of class, he drew the following diagram on the board to tell the students whether to expect a full assignment, a partial assignment, or no assignment for the following week.



The edges of the diagram are labeled by the probability that one state will follow the other. The successive iteration of this process from week to week is what is called a *discrete-time random walk*.

For each of the parts below, please report your answer to two decimal places.

(a) Construct the pdit pgate (see problem 1.1) that corresponds to this diagram.

(b) What is the probability that there will be a full assignment two weeks from now if there is no assignment this week?

(c) What is the probability that there was no assignment the first week, if all you know is that two weeks later there was a full assignment?

(d) What is the probability that there will be a partial assignment 16 weeks from now if there is a full assignment this week? (Hint: Diagonalize!)

(e) What input pdit state is invariant under the action of the pgate describing assignments? (Hint: Diagonalize!)

(f) What does the pgate P^n converge to as $n \to \infty$?

Extra Credit Problem

1.4 Don't misunderestimate the power of language

Some politicians seem to speak in a way that suggests that they draw one word after the other in a mindless fashion, as though they were just sampling from a probability distribution. Write a computer program that will read in a sample of text and store the transition probabilities that one word follows the other. Feel free to use whatever data structure you deem most appropriate for this task, although be careful—if you don't think about this carefully you could run out of computer memory when reading in a large sample of text. Your data structure is essentially holding a representation of a large pdit pgate, where d is equal to the number of distinct words in the text. Have the program then use that data structure and a random starting "seed word" drawn from the text to generate an output stream of text using those probabilities. Be sure to include one "word" that is an "end of text" word so that your output has a chance of terminating. It is also probably a good idea to allow punctuation to be considered part of the words being sampled to give at least some semblance of structure to the generated text.

E-mail your program along with a sample input text and the output text it generates. There should be a way for your code to accept an ASCII test file as input for the grader to check your program. Please include instructions as to how your program accepts such an input and how it generates an output.

Please write your program in Matlab or C/C++. If you'd like to use another language, you may do so only if you check with the grader first.